31

October 14, 2003

Filed via E-Mail

Public Information Room
Office of the Comptroller of the
Currency
250 E Street, S.W., Mail Stop 1-5
Washington, DC 20219
Docket No. 03-18

Ms. Jennifer J. Johnson, Secretary
Board of Governors of the Federal
Reserve System
20th Street and Constitution Ave., N.W.
Washington, DC 20551
Docket No. OP-1155

Mr. Robert E. Feldman, Executive
Secretary
Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, N.W.
Washington, DC 20429

Regulation Comments, Chief
Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
Attn: No. 03-35

RE: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Dear Sirs and Madams:

Mellon Financial Corporation, Pittsburgh, Pennsylvania, appreciates the opportunity to comment on the proposed Guidance issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision ("the Agencies"), interpreting Section 501(b) of the Gramm-Leach-Bliley Act ("the Act"). We offer the following comments for your consideration:

Guidance Should Be Goal-Oriented. Without question, the security, confidentiality, and integrity of the information financial institutions have about their customers are matters of the utmost importance. For this reason, it is essential that institutions, in developing measures to protect customer information, maintain the ability to respond to rapidly evolving technology and market conditions. Regulatory prescriptions which are overly detailed and specific will inhibit institutions' flexibility to innovate in the area of information security; this will actually *reduce* security, while imposing unnecessary costs on institutions and their customers. Therefore, we believe the Guidance should be goal-oriented, setting forth the objectives to be attained, rather than process-oriented.

We believe the Agencies are on the right track in adopting a risk-based approach to determining when it is appropriate to notify customers of a security incident. Our understanding of the Guidance as proposed is that the requirement to give notice to customers is tailored to those situations in which there is a significant likelihood that meaningful loss will occur as a result of the incident.

Flagging and Securing Accounts. However, in certain respects the proposed Guidance is too prescriptive, and not entirely consistent with this risk-based approach. This is especially true in Sections II.D.1 and 2, which talk about "flagging" and "securing" accounts. We are not entirely certain what is meant by these terms; at the very least, they require clarification. However, regardless of what precise actions were intended, we think it is inadvisable for the Guidance to prescribe responses to security incidents with this level of detail.

The ability to "flag" accounts on a system is likely to require a large financial investment for most institutions – an investment which may be unnecessary, as institutions already have well-established mechanisms for responding to potential fraudulent activity on customers' accounts. Money spent on developing the capability to flag accounts is money not available for more productive purposes, such as enhancements to minimize exposure of information systems and networks to intrusion and unauthorized access. Institutions should have the flexibility to respond to security incidents in the manner that reflects industry best practices and state of the art technology; they should not be tied down to a specific methodology. Similarly, if one assumes that "securing" an account means freezing all account activity, such action may be detrimental to the customer, while being less effective than simply closing the account and opening a new one. We strongly believe that any such rigid rules about how to deal with the wide variety of possible security incidents that may occur are misplaced in this Guidance. If it is considered desirable to retain references to flagging or securing accounts, we suggest including the words "where appropriate" in order to give institutions the flexibility to choose the most effective solutions to problems.

In particular, the requirement in II.D.2 that the institution and the customer "agree on a course of action" is unrealistic and unworkable. An institution must have the ability to implement the best solution to a problem, even when customers may not necessarily be in agreement. Unfortunately, not all customers always understand what course of action is in their best interests, and some may refuse to agree to measures that are required for their own protection. Further, when a security incident involves a large number of accounts, an institution must have the ability to react expeditiously and efficiently, which means implementing a uniform response that solves the problem for all accounts at one time. A requirement to secure the consent of thousands of customers to the issuing of new credit cards, for example, would be impossible to comply with, and attempts to comply would entail tremendous expense and delay which would serve no obvious purpose. Any suggestion that an institution's response to a security breach must be a collaborative decision involving each impacted customer is completely unrealistic and should be avoided.

Customer Notification. Regarding the customer notification requirement, as noted above we believe that the Agencies have taken a commendably practical approach by

tying the need to give notice to the risk of harm to the customer. However, we have a number of concerns about this section of the Guidance:

(1) The definition of "sensitive customer information" sets forth two lists of specific information items, and suggests that any combination of an item from "List 1" and an item from "List 2" constitutes "sensitive information." The literal result of this process is that a person's name and account number together constitute "sensitive information," notwithstanding that name and account number combinations are often widely known, *e.g.*, through the use of checks, credit cards, and the like. We suggest that the second list be modified, such as by saying "account number in combination with any required security code, access code, or password that would permit access to an individual's account." (This is the approach taken by California Civil Code §1798.82(e) in defining "personal information.)

(2) If a definition of "sensitive data" is retained, publicly available information, meaning information that is lawfully made available to the general public from federal, state, or local government records, should be excluded from the definition.

(3) It should be made clear in II.D.3 that an institution is encouraged to take the time it reasonably needs to assess the risk resulting from a security incident and provide its customer-facing employees with the necessary information about the situation and proposed remediation prior to making the determination to notify customers. This approach ensures that customer-facing employees can communicate with customers in such a fashion as to address anxieties caused by receiving the notices. As a result, customers will be less likely to unnecessarily change passwords, cancel accounts, or take other actions burdensome to themselves after receiving a notification.

(4) On the other hand, frequent notices are likely to make customers less responsive, so that they fail to take action when it is really necessary. Therefore, "timely" notice should not be interpreted to require institutions to forgo thorough investigation as a prerequisite to notification. It is particularly important that if a vulnerability is discovered, an institution does not postpone remediation actions

because of a requirement to notify customers. Postponing remediation could risk further exploitation of the vulnerability.

(5) The Guidance should include a provision (similar to that found in California Civil Code §1798.82(c)) that allows a delay in notification to customers if a law enforcement agency determines that the notification will impede a criminal investigation.

(6) Certain aspects of the customer notice prescribed by Section II.D.3.b may increase financial institutions' costs dramatically. There are tangible costs associated with delivery of a notice. If an incident affects a large portion of the customer base of the typical financial institution or even a large portion of the customer base for some products of an institution, the costs could be enormous. In addition, the costs of meeting the requirements of footnote 17 (requiring a sufficient number of appropriately trained employees to be available to answer customer inquiries and provide assistance) could also be substantial.

A less prescriptive model for customer notices would alleviate the financial and practical burden that the proposed Guidance will impose upon institutions. In particular:

- Section II.D.3 should be changed to say, "*Key Elements:* In addition, the notice should, where appropriate...."

- The requirement to inform affected customers that the institution will assist the customer to correct and update information in any consumer credit report relating to the customer should be deleted. Requiring financial institutions to add this information in their notice to customers goes beyond the requirements of the Fair Credit Reporting Act and imposes a potentially costly obligation on financial institutions.

- The Fair Credit Reporting Act and numerous other federal laws already provide consumers substantial protection against fraudulent transactions. Therefore, we do not believe the "Optional Elements" in Section II.3 serve

any useful purpose. Further, those additional elements may be perceived as mandatory by customers and institutions. Many of these elements are onerous, costly, and inappropriate in a number of circumstances. For example, the suggestion that an institution offer to assist a customer in notifying the nationwide credit reporting agencies of an incident and further offer to assist customers in placing a fraud alert in the customers' reports is an example of a highly costly element that should be left outside the scope of this Guidance.

- The arguments set forth above also apply to the suggestion in the "Optional Elements" section of the proposed Guidance that an institution offer to subscribe a customer to a subscription service free of charge for a period of time (these subscription services provide customers notification of requests that have been made for a customer's credit report). We strongly believe that this suggestion is misplaced in the proposed Guidance and should be deleted.

Notification to Federal Regulators. The proposed Guidance mandates in Section II.B that an institution promptly notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers. First, we are uncertain what purpose is served by requiring additional notification when an institution is already required to file a Suspicious Activity Report.

Further, unauthorized access that "could" result in inconvenience is an extremely low threshold. Under this standard, virtually every incident may require notification. We understand that regulators need to be informed of significant incidents, but notification should only be required when an incident poses a significant risk of substantial harm to a significant number of customers.

* * *

In conclusion, we wish to emphasize that Mellon, like other members of the financial services industry, wishes to protect the legitimate security interests of consumers in a manner consistent with the goals of Congress as expressed in the Act. It is our hope

that these comments will be helpful to the Agencies in fashioning final Guidance to promote those goals.

If you would care to discuss any of the comments in this letter, please feel free to call the undersigned at 412-234-1537 or Charles F. Miller at 412-234-0564.

Sincerely,

Michael E. Bleier

cc: George Orsino
Frank Riccardi